REMARKS

In view of the above amendments the following remarks, and the After Final Amendment previously filed on April 20, 2009, reconsideration and further examination are respectfully requested.

I. Interview

The Applicants would like to thank Examiner King for granting and conducting a telephone interview on March 3, 2009 in connection with the above-identified application.

Prior to the interview the Examiner kindly reviewed the Applicants' proposed claims. During the interview, the Examiner suggested that the Applicants consider further amending the claims to clarify that just one comparison computation value is generated from the one message. Specifically, the Examiner indicated that if such amendments are submitted, then he will be required to search other portions of the Yamamichi reference, as well as search for additional prior art that discloses the above-mentioned distinguishing limitation, because it appeared to the Examiner that the presently identified portions of Yamamichi fail to disclose or suggest the distinguishing limitation mentioned above.

As a result, the Examiner indicated that, if such amendments were made, then he would reconsider his rejection of independent claims 1, 3, 7, 11, 12, 14 and 15 when a formal Response is filed.

II. Amendments to the Claims

Based on the above-mentioned interview, **in the After Final Amendment previously filed on April 20, 2009** independent claims 1, 3, 7, 11, 12, 14 and 15 have been amended to overcome the Yamamichi reference cited in the Office Action of January 23, 2009 by including the additional amendments suggested by the Examiner.

Furthermore, **by this present amendment** new dependent claims 17-19 have been added. Support for the limitations recited in new claims 17-19 can be found, at least, in item (3) spanning pages 26 and 27 of the previously submitted substitute specification.

III. Claim Objection

Claim 7 was objected to for reciting "mesasage," rather than "message." **In the After Final Amendment previously filed on April 20, 2009** claim 7 has been amended to replace the term "mesasage" with the term "message." As a result, Applicants respectfully request that the Examiner withdraw this objection.

IV. Claim Rejection under 35 U.S.C. § 103(a)

Claims 1, 2, 7-10, 14 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Yamamichi et al. (U.S. 2002/0116612) and Olson et al. (U.S. 2003/0226007). This rejection is believed clearly inapplicable to independent claims 1, 3, 7, 11, 12, 14 and 15 and the claims that depend therefrom for the following reasons.

Independent claim 1 recites an encryption system including a computation unit operable

to perform a one-way operation on one message (the one message is used to generate a plurality of encrypted messages) to generate only one comparison computation value from the one message. Further, claim 1 recites that the system includes a transmission unit operable to transmit, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value. Moreover, claim 1 recites that the system includes a judging unit operable to compare each of the decryption computation values with the received one comparison computation value, wherein (i) when at least one of the plurality of the decryption computation values matches the one received comparison computation value, the judging unit outputs a decrypted message as a correct decrypted message, and (ii) when none of the decryption computation values matches the one received comparison computation value, the judging unit determines that there is a decryption error.

In summary, independent claim 1 recites generating only one comparison computation value from the one message that is used to generate a plurality of encrypted messages, such that the one comparison computation value is compared to a plurality of decryption computation values obtained from the plurality of encrypted messages to determine whether or not to output a decrypted message or a decryption error.

Initially, please note that the above-described 35 U.S.C. § 103(a) rejection relies on Yamamichi for teaching the features of the claimed "generation of the comparison computation value." However, Applicants respectfully submit that Yamamichi fails to disclose or suggest the above-noted "generation of only one comparison computation value from the one message," as recited in independent claim 1.

Rather, Yamamichi, as acknowledged by the Examiner during the above-mentioned telephone interview, merely teaches that a one-way operation unit performs a hash function on each individually received text m' (there are multiple received texts m_1', m_2', ... etc. which are generated from a single message), to generate a hash value for each individually received text m_1', m_2', ... etc (see paragraphs [0011]-[0015] and [0098]). In other words, Yamamichi teaches that from one single message, multiple texts are generated and from each of the multiple texts an individual hash value is obtained.

Applicants note that the rejection on page 7 of the Office Action dated January 23, 2009 rejects the independent claims by combining paragraphs [0011]-[0016] with paragraphs [0100] and [0101] of Yamamichi. Applicants respectfully disagree that the features of paragraphs [0011]-[0016] and the features of paragraphs [0100] and [0101] can be combined, as taught by Yamamichi, for the following reasons.

Paragraphs [0011]-[0016] of Yamamichi teach that (i) the encrypting apparatus encrypts one "plaintext" to generate a plurality of "ciphertext," (ii) the decrypting apparatus decrypts a plurality of "ciphertext" to generate a plurality of decrypted text, and (iii) the decrypting apparatus determines that a decryption error has occurred when a single component in one of the decrypted texts is different from a corresponding component of the other decrypted texts. The purpose of the above-described disclosure of Yamamichi is to increase a volume of communication. Applicants also note that this above-mentioned disclosure of Yamamichi does not teach the use of a hash value.

Paragraphs [0100] and [0101] of Yamamichi teach that the comparison unit 205 compares the function value h(m) and the function value h(m'), and judges whether the value

h(m) matches the value h(m'). More specifically, Yamamichi teaches that one has value, h(m), is generated for one ciphertext, and one has value, h(m'), is generated for one decrypted text, such that the hash value generated for the ciphertext is compared with the hash value generated for the decrypted text. Applicants note that the purpose of the above-mentioned disclosure of Yamamichi is to decrease the volume of communication.

In view of the above, Applicants submit that the disclosure of paragraphs [0011]-[0016] cannot be combined with the disclosure of paragraphs [0100] and [0101], since the purpose of the disclosure of paragraphs [0011]-[0016] is to increase the volume of communication, and, in contrast, the purpose of the disclosure of paragraphs [0100] and [0101] is to decrease the volume of communication. For this reason alone, Yamamichi fails to disclose or suggest the above-identified distinguishing features, as recited in claim 1.

Furthermore, in view of the above, it is clear that Yamamichi requires that multiple hash values are generated from one single message, but fails to disclose or suggest generating only one comparison computation value from the one message that is used to generate a plurality of encrypted messages, such that the one comparison computation value is compared to a plurality of decryption computation values obtained from the plurality of encrypted messages to determine whether or not to output a decrypted message or a decryption error, as required by claim 1.

In other words, as agreed upon by the Examiner, Yamamichi is silent on generating a hash value (i.e., comparison computation value) from the one message in a situation where a plurality of encrypted messages are generated from the one message and the one comparison

computation value is compared to a plurality of decryption computation values obtained from the plurality of encrypted messages, as required by claim 1.

Therefore, because of the above-mentioned distinctions it is believed clear that claim 1 and claim 2 that depends therefrom would not have been obvious or result from any combination of Yamamichi and Olson.

Furthermore, there is no disclosure or suggestion in Yamamichi and/or Olson or elsewhere in the prior art of record which would have caused a person of ordinary skill in the art to modify Yamamichi and/or Olson to obtain the invention of independent claim 1. Accordingly, it is respectfully submitted that independent claim 1 and claim 2 that depends therefrom are clearly allowable over the prior art of record.

Independent claims 3, 7, 11, 12, 14 and 15 are directed to a transmission apparatus, a reception apparatus, a transmission method, a transmission program, a reception method, and a reception program, respectively and each recite features that correspond to the above-mentioned distinguishing features of independent claim 1. Thus, for the same reasons discussed above, it is respectfully submitted that claims 3, 7, 11, 12, 14 and 15 and the claims that depend therefrom are allowable over the prior art of record.

IV. Conclusion

In view of the above amendments and remarks, and the After Final Amendment previously filed on April 20, 2009, it is submitted that the present application is now in condition for allowance and an early notification thereof is earnestly requested. The Examiner is invited to contact the undersigned by telephone to resolve.

The Commissioner is authorized to charge any deficiency or to credit any overpayment associated with this communication to Deposit Account No. 23-0975, with the EXCEPTION of deficiencies in fees for multiple dependent claims in new applications.

Respectfully submitted,

Yuichi FUTA et al.

By: /Andrew L. Dunlap/
2009.06.23 16:18:44 -04'00'

Andrew L. Dunlap
Registration No. 60,554
Attorney for Applicants

ALD/led
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
June 23, 2009